

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-219853

(43)Date of publication of application : 18.08.1995

(51)Int.Cl.

G06F 12/14

(21)Application number : 06-008199

(71)Applicant : NEC ENG LTD

(22)Date of filing : 28.01.1994

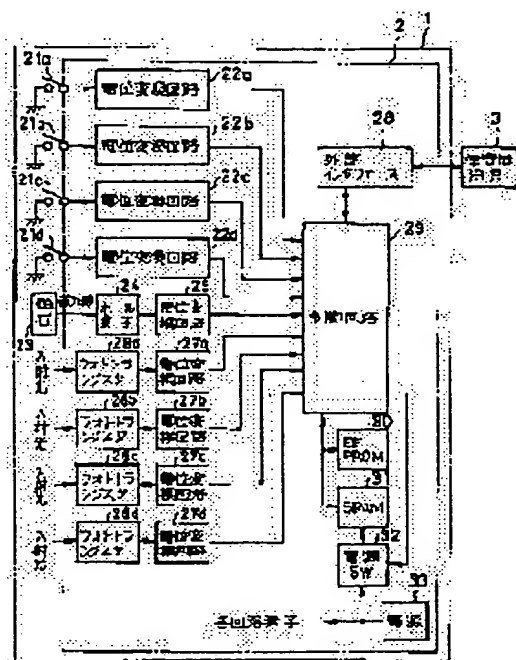
(72)Inventor : SAKAKIBARA OSAMU

(54) TERMINAL EQUIPMENT

(57)Abstract:

PURPOSE: To recognize an illicit access without using any mechanical means.

CONSTITUTION: The spring-shaped metallic parts 21a-21d and the potential converting circuits 22a-22d are provided on a printed circuit board 2 and electrically detect the dismantling of a terminal equipment 1. Meanwhile a magnet 23, a Hall element 24 and a potential converting circuit 25 which are attached to a housing magnetically detect the dismantling of the equipment 1. Furthermore the phototransistors 26a-26d and the potential converting circuits 27a-27d optically detect the dismantling of the equipment 1 respectively. A control circuit 29 decides whether the reasons of notifications are due to the accidental troubles such as the falls, etc., or the illicit dismantling done by a malicious third party based on the order and combinations of notifications given from the circuits 22a-22d, 25 and 27a-27d. If the illicit dismantling is decided, the circuit 29 erases the secret information stored in an EEPROM 30 and an SRAM 31. Then the circuit 29 certifies a maintenance jig 3 with each other through an external interface 28.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平7-219853

(43) 公開日 平成7年(1995)8月18日

(51) Int.Cl.⁶

G 0 6 F 12/14

識別記号

3 2 0 D

庁内整理番号

F I

技術表示箇所

審査請求 未請求 請求項の数 4 O L (全 11 頁)

(21) 出願番号 特願平6-8199

(22) 出願日 平成6年(1994)1月28日

(71) 出願人 000232047

日本電気エンジニアリング株式会社
東京都港区芝浦三丁目18番21号

(72) 発明者 榊原 修

東京都港区西新橋三丁目20番4号 日本電
気エンジニアリング株式会社内

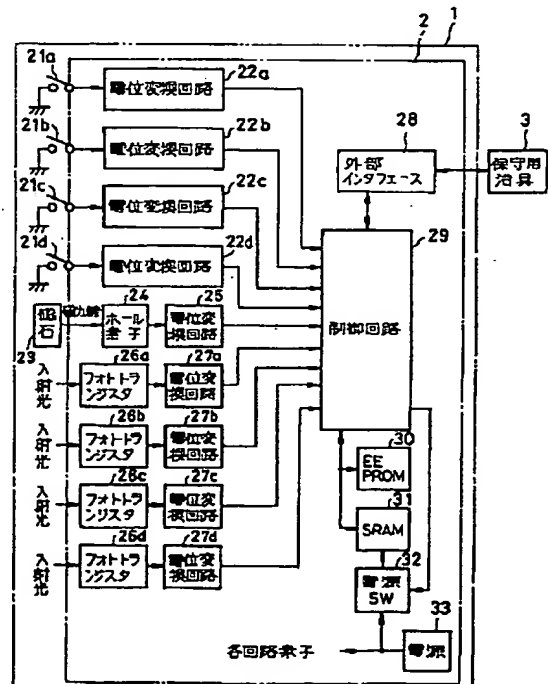
(74) 代理人 弁理士 京本 直樹 (外2名)

(54) 【発明の名称】 端末装置

(57) 【要約】

【目的】 機械的な手段を用いることなく、不正アクセスの認識を可能とする。

【構成】 プリント配線基板2上のパネ状の金具21a～21d及び電位変換回路22a～22dは端末装置1の解体を電氣的に検出する。筐体に取り付けた磁石23とホール素子24と電位変換回路25とは端末装置1の解体を磁氣的に検出する。フォトトランジスタ26a～26dと電位変換回路27a～27dとは端末装置1の解体を光学的に検出する。制御回路29は電位変換回路22a～22d, 25, 27a～27dからの通知の順序及び組合せ等によって通知原因を落下等の偶発事故によるものか悪意の第三者の不正解体によるものかを判断する。制御回路29は悪意の第三者の不正解体によるものと判断すると、EEPROM30及びSRAM31に記憶された秘密情報を消去する。制御回路29は外部インタフェース28を通じて保守用治具3との間で相手認証を行う。



【特許請求の範囲】

【請求項1】 秘密情報を記憶するメモリを含む電子回路が搭載されたプリント配線基板と、前記プリント配線基板を収納する外部筐体と、前記電子回路に対する外部からのアクセス許可要求の適否を判定する判定手段と、前記外部筐体の解体の有無を検出する複数の検出手段と、前記判定手段の判定結果及び前記複数の検出手段各々の検出結果に基づいて前記外部筐体の不正な解体か否かを判断する判断手段と、前記判断手段が前記外部筐体の不正な解体と判断したときに前記秘密情報を前記メモリから消去する手段とを含むことを特徴とする端末装置。

【請求項2】 前記判定手段は、相手認証方式によって前記アクセス許可要求の適否を判定するよう構成されたことを特徴とする請求項1記載の端末装置。

【請求項3】 前記複数の検出手段は、前記外部筐体の解体を電氣的に検出する第一の検出手段と、前記外部筐体の解体を光學的に検出する第二の検出手段と、前記外部筐体の解体を磁氣的に検出する第三の検出手段とを含むことを特徴とする請求項1または請求項2記載の端末装置。

【請求項4】 前記判断手段は、前記判定手段が前記アクセス許可要求なし及び前記アクセス許可信号の否のうち一方を検出したときに前記第一の検出手段と前記第二の検出手段と前記第三の検出手段とにおける夫々の検出状態及びその順序に応じて前記外部筐体の不正な解体か否かを判断するよう構成されたことを特徴とする請求項3記載の端末装置。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は端末装置に関し、特に移動体通信端末装置の秘匿情報漏洩防止方式に関する。

【0002】

【従来の技術】従来、この種の秘匿情報漏洩防止方式においては、装置筐体が不正に破壊もしくは解体され、内部の電子回路内のメモリに記憶されている秘密情報が不正に取出されるのを防止するために、装置筐体が不正に破壊もしくは解体されるのを検知したときにメモリ内の秘密情報を消去するよう構成されている。

【0003】すなわち、図7に示すように、通常、錠45が取付けられている装置筐体の扉（図示せず）及び錠45に夫々取付けられた柱状突起41、46がマイクロスイッチ43、48のパネ板42、47を押圧することで、マイクロスイッチ43、48がオン状態となっている。

【0004】内部の電子回路にアクセスする場合に錠45を開錠すると、柱状突起46が上方に離れてマイクロスイッチ48のパネ板47が解放され、マイクロスイッチ48がオフ状態となる。アクセス開始検出回路49はマイクロスイッチ48がオフ状態となったことを検出す

ると、判定回路50にアクセス開始信号102を出力する。

【0005】この後に、装置筐体の扉を開けると、柱状突起41が上方に離れてマイクロスイッチ43のパネ板42が解放され、マイクロスイッチ43がオフ状態となる。内部アクセス検出回路44はマイクロスイッチ43がオフ状態となったことを検出すると、判定回路50に内部アクセス信号101を出力する。

【0006】判定回路50は上述の如く、錠45が開錠されてから装置筐体の扉が開けられると、アクセス開始検出回路49からアクセス開始信号102が入力された後に内部アクセス検出回路44から内部アクセス信号101が入力されるので、不正アクセス信号103を抹消信号発生回路51に出力しない。よって、抹消信号発生回路51からメモリ52に抹消信号104が出力されないため、メモリ52に記憶されている秘密情報が消去されることはない。

【0007】これに対して、錠45を開錠することなく、装置筐体の扉が開けられると、内部アクセス検出回路44から判定回路50に内部アクセス信号101が出力される。

【0008】判定回路50はアクセス開始検出回路49からアクセス開始信号102が入力されていないにもかかわらず、内部アクセス検出回路44から内部アクセス信号101が入力されるので、不正アクセスがあったとして不正アクセス信号103を抹消信号発生回路51に出力する。

【0009】よって、抹消信号発生回路51からメモリ52に抹消信号104が出力されるので、この抹消信号104に応答してメモリ52に記憶されている秘密情報が消去される。

【0010】上述した秘匿情報漏洩防止方式の技術については、特公平1-47059号公報に詳述されている。

【0011】

【発明が解決しようとする課題】上述した従来の秘匿情報漏洩防止方式では、錠やマイクロスイッチ等の機械的な手段を用いて内部の電子回路への不正アクセスを検出しているため、装置筐体の構成材料である金属やプラスチック等に対して可透過の性質を持つX線や超音波等を使用し、装置筐体外部から不正アクセスを検出する構造を解析する手段を有する悪意の第三者に対しては不正アクセスを阻止することができない。

【0012】また、アクセスの正当性確認のために錠やマイクロスイッチ等の機械的な手段を使用するため、装置に対して容積や重量の増大を招く。さらに、一般的に錠と鍵との組合せは10の4乗程度であるため、不正開錠の恐れが高い。

【0013】さらにまた、落下事故等によって装置が機械的に破損したり、荷重を受けたときに不正アクセスと

誤認して秘密情報を消去する場合があります、実使用上問題のない軽微な筐体の損傷であっても修理や保守を行わない限り、機器の運用が不可能となる。

【0014】そこで、本発明の目的は上記の問題点を解消し、機械的な手段を用いることなく、不正アクセスの認識を可能とすることができる端末装置を提供することにある。

【0015】

【課題を解決するための手段】本発明による端末装置は、秘密情報を記憶するメモリを含む電子回路が搭載されたプリント配線基板と、前記プリント配線基板を収納する外部筐体と、前記電子回路に対する外部からのアクセス許可要求の適否を判定する判定手段と、前記外部筐体の解体の有無を検出する複数の検出手段と、前記判定手段の判定結果及び前記複数の検出手段各々の検出結果に基づいて前記外部筐体の不正な解体か否かを判断する判断手段と、前記判断手段が前記外部筐体の不正な解体と判断したときに前記秘密情報を前記メモリから消去する手段とを備えている。

【0016】

【実施例】次に、本発明の一実施例について図面を参照して説明する。

【0017】図1は本発明の一実施例の構成を示すブロック図である。図において、端末装置1内部に載置されたプリント配線基板2には端末装置1の解体を電気的に検出するためのバネ状の金具21a～21dと、端末装置1の解体を磁気的に検出するためのホール素子24と、端末装置1の解体を光学的に検出するためのフォトトランジスタ26a～26dとが搭載されている。

【0018】バネ状の金具21a～21dは端末装置1の筐体（図示せず）が組立て状態にあるときにグランドと導通状態となり、筐体が解体されるときにグランド電位とは異なる電位を持つことになる。

【0019】プリント配線基板2上の電位変換回路22a～22d各々は対応するバネ状の金具21a～21dの電位変化を検出し、検出／非検出の二値信号に変換して制御回路29に通知する。

【0020】ホール素子24はプリント配線基板2の上面中央に実装され、プリント配線基板2の上面に対向する端末装置1の筐体の内面中央に載置された磁石23の磁界変化を検出し、その磁界変化を電気信号に変換して出力する。

【0021】電位変換回路25はホール素子24で電気信号に変換された磁界変化を検出し、検出／非検出の二値信号に変換して制御回路29に通知する。尚、ホール素子24は磁界指向性がよく、磁界の強さに対して出力値が電位変換回路25の電源電圧まで飽和しないものが好ましい。

【0022】これによって、端末装置1の製造時に正規組立状態でのホール素子24の出力値をEEPROM3

0に記録することで、その出力値以上の磁界の強さを検出した場合に端末装置1の筐体の解体の可能性があると判断することが可能となる。

【0023】フォトトランジスタ26a～26dはプリント配線基板2の上面及び下面に夫々2つつつ実装されており、プリント配線基板2の上面及び下面各々の同一面側では上部側及び下部側に振り分けられて実装されている。

【0024】この場合、同一面側の上部側及び下部側に実装されたフォトトランジスタはその二つの素子の受光感度半値角の延長線がプリント配線基板2と相対する筐体の内壁との間の空間で交わることが望ましい。

【0025】また、プリント配線基板2の短辺側の端部にフォトトランジスタを搭載する場合に、そのフォトトランジスタの受光感度半値角は90°に近ければ近いほどよい。

【0026】フォトトランジスタ26a～26dは端末装置1の筐体が解体されて外部から光線が照射されると、その出力値を変化させる。電位変換回路27a～27dは対応するフォトトランジスタ26a～26dの出力の変化を検出し、検出／非検出の二値信号に変換して制御回路29に通知する。

【0027】制御回路29は電位変換回路22a～22d、25、27a～27dからの通知を受けると、それら通知の順序及び組合せ等によって通知原因を落下等の偶発事故によるものか悪意の第三者の不正解体によるものかを判断する。制御回路29は悪意の第三者の不正解体によるものと判断すると、EEPROM30及びSRAM31に記憶された秘密情報を消去する。

【0028】EEPROM30には秘密情報として、回線網（図示せず）との接続に必要なパラメータ、端末装置使用者の個人データ、保守用治具3の相手認証に必要な情報等が記憶されている。

【0029】また、SRAM31には秘密情報として、発呼先登録、受信内容記憶、発呼・着呼等通話記録、課金情報・記録等が記憶されている。

【0030】EEPROM30及びSRAM31は制御回路29に接続され、必要に応じて制御回路29から書き込み及び読出しが行われる。ここで、本発明の一実施例ではEEPROM30及びSRAM31を併記したが、端末装置1の回路構成によってはどちらか一方か、あるいは類似の記憶素子であってもよい。

【0031】また、制御回路29は外部インタフェース28を介して保守用治具3と通信可能となっており、端末装置1の筐体の保守解体時には保守用治具3から端末装置1に対する相手認証が行われる。

【0032】電源スイッチ（SW）32は電源33からSRAM31に対する電源を制御回路29からの制御信号に応じてオンオフ制御する。電源33はSRAM31に対して電源を供給するとともに、プリント配線基板2

上の各回路素子に電源を供給する。

【0033】図2は本発明の一実施例の組立図であり、図3は組立て状態における図2のAA線に沿う矢視方向の断面図であり、図4は組立て状態における図2のBB線に沿う矢視方向の断面図である。

【0034】これら図1～図4を用いて端末装置1の組立てを順を追って説明する。まず、プリント配線基板2に対して筐体前面部4及び筐体後面部5を固定するためのネジ穴部周辺を除いた端部全周域にベリリウム銅やリン青銅等のバネ性を持った導電性金属からなる金具8a～8lを嵌め込む。このとき、プリント配線基板2のグラ

ンドと金具8a～8lとは電氣的に導通状態となる。【0035】また、上記と同様の導電性金属からなるバネ状の金具21a～21dはプリント配線基板2の端部のグラ

ンドと導通している銅箔部の上に被さるように、かつ銅箔部に接触しない状態でプリント配線基板2のパターンに半田付けされ、電位変換回路22a～22dの入力に夫々接続される。【0036】プリント配線基板2をネジ9a、9bで筐体後面部5にネジ止めすると、バネ状の金具21b、21dは夫々筐体後面部5の内面に押し付けられ、プリント配線基板2の銅箔部に接触する。よって、バネ状の金具21b、21dはプリント配線基板2のグラ

ンドと電氣的に導通状態となる。【0037】また、筐体後面部5の内面は全体的にアルミニウム蒸着によって電氣的に導通可能な状態にあるため、ネジ9a、9bでプリント配線基板2が筐体後面部5にネジ止めされると、プリント配線基板2のグラ

ンドと筐体後面部5の内面とは同一電位となる。【0038】次に、密閉用ゴムパッキン7を筐体後面部5の筐体前面部4との接合部に嵌め込み、筐体前面部4の上部の爪4aを筐体後面部5の上部の爪5aに引掛け、バネ状の金具21a、21cを夫々筐体前面部4の内面によってプリント配線基板2の銅箔部に接触させた状態で、ネジ9e、9fによって筐体後面部5を筐体前面部4にネジ止めする。

【0039】その後、ネジ9c、9dによって筐体後面部5を筐体前面部4にネジ止めする。ここで、筐体前面部4の内面は筐体後面部5の内面と同様にアルミニウム蒸着されているため、プリント配線基板2のグラ

ンドと筐体前面部4の内面とは同一電位となる。【0040】したがって、筐体後面部5側と同様に、プリント配線基板2のグラ

ンドと筐体後面部5の内面とバネ状の金具21a、21cとは同一電位となる。尚、筐体前面部4の内面中央には磁石23が、プリント配線基板2上のホール素子24に対向する位置に取付けられている。【0041】最後に、筐体後面部5の溝部5b、5cに夫々電池ケース6の爪6a、6bを嵌め込むことによ

で、端末装置1が動作可能となる。

【0042】尚、端末装置1が動作すると、LCD（図示せず）上に表示されたメッセージ等をLCDカバーガラス10を通して見る事が可能になるとともに、キートップ11を介してキー入力を行うことができる。

【0043】図5は図2の金具8aを示す斜視図であり、図6は図5のCC線に沿う矢視方向の断面図である。これらの図において、金具8aはコの字形状となっており、互いに対向する2つの面8a-1、8a-2と底面8a-3とからなっている。

【0044】金具8aはプリント配線基板2に嵌め込むために、その開口側の面8a-1、8a-2の間隔が底面8a-3側の面8a-1、8a-2の間隔よりも狭くなるように、面8a-1、8a-2はテーパ状に底面8a-3につながっている。

【0045】また、底面8a-3側の面8a-1、8a-2の間隔はプリント配線基板2の厚さと同じとなっているため、金具8aをプリント配線基板2に嵌め込むだけで金具8aとプリント配線基板2との間の電氣的導通を確保することができる。

【0046】尚、図示していないが、他の金具8b～8lも金具8aと同一形状となっており、金具8b～8lをプリント配線基板2に嵌め込むだけで金具8b～8lとプリント配線基板2との間の電氣的導通を確保することができる。

【0047】図7は図2のバネ状の金具21aの取付け状態を示す斜視図であり、図8は図7のDD線に沿う矢視方向の断面図である。これらの図において、バネ状の金具21aはプリント配線基板2上に載置され、その一端がプリント配線基板2の挿入部品半田付け用導通貫通穴13に半田付けされている。

【0048】また、バネ状の金具21aは折曲げ部分aで、その他端がプリント配線基板2上の銅箔部12に接触しないように折曲げられている。バネ状の金具21aの他端は筐体後面部5がネジ9c～9fによって筐体前面部4にネジ止めされると、筐体前面部4の内面によってプリント配線基板2上の銅箔部12に押付けられ、プリント配線基板2のグラ

ンドと電氣的に導通状態となる。【0049】尚、図示していないが、バネ状の金具21b～21dも上記のバネ状の金具21aと同様に、一端がプリント配線基板2の挿入部品半田付け用導通貫通穴13に半田付けされ、かつ他端がプリント配線基板2上の銅箔部12に接触しないように折曲げ部分aで折曲げられている。

【0050】図9は図1の磁石23及びホール素子24による端末装置1の解体の磁氣的な検出動作を示す図である。図9(a)はプリント配線基板2と筐体前面部4と筐体後面部5とを組立てる前の状態を示しており、図9(b)はプリント配線基板2と筐体前面部4と筐体後

面部5とを組立てた後の状態を示している。

【0051】これらの図において、磁石23及びホール素子24は互いに対向するように、夫々筐体前面部4の内面中央及びプリント配線基板2の上面中央に設置されている。尚、磁石23は筐体前面部4の内面に取付けられたキースイッチ押え板14に当接して設置されている。

【0052】プリント配線基板2と筐体前面部4と筐体後面部5とを組立てると、磁石23及びホール素子24は常に当接あるいは接近した状態となり、ホール素子24は磁石23の磁界を検出し、一定の信号を出力する。

【0053】この状態で、端末装置1が解体されると、磁石23がホール素子24における磁界検出範囲から外れてしまうので、ホール素子24は磁石23の磁界変化を検出し、その磁界変化を電気信号に変換して出力する。これによって、端末装置1の解体を磁氣的に検出することが可能となる。

【0054】図10は図1のバネ状の金具21a～21dによる端末装置1の解体の電氣的な検出動作を示す図である。図10(a)はプリント配線基板2と筐体前面部4と筐体後面部5とを組立てる前の状態を示しており、図10(b)はプリント配線基板2と筐体前面部4と筐体後面部5とを組立てた後の状態を示している。

【0055】これらの図において、プリント配線基板2と筐体前面部4と筐体後面部5とを組立てる前にはバネ状の金具21a、21b各々の他端がプリント配線基板2上の銅箔部12に接触しないようになっている。

【0056】プリント配線基板2と筐体前面部4と筐体後面部5とを組立てると、バネ状の金具21a、21b各々の他端は筐体前面部4及び筐体後面部5の内面によってプリント配線基板2上の銅箔部12に押付けられ、プリント配線基板2のグラウンドと電氣的に導通状態となる。

【0057】この状態で、端末装置1が解体され、筐体前面部4及び筐体後面部5がプリント配線基板2から取外されると、バネ状の金具21a、21b各々の他端がプリント配線基板2上の銅箔部12から離れるので、バネ状の金具21a、21bの電位が変化する。

【0058】このバネ状の金具21a、21bの電位変化を検出することで、端末装置1の解体を電氣的に検出することが可能となる。

【0059】図11は図1の端末装置1における相手認証方法の手順を示すフローチャートである。この図11を用いて端末装置1における相手認証方法の手順について以下説明する。

【0060】ここで、EEPROM30には保守用治具3の相手認証を行うための情報として、端末装置個別番号R(相手認証方式における検証者側乱数)と、保守用治具識別番号U(相手認証方式における証明者側乱数)と、相手認証確認用一方関数 $f(R, U)$ とが予め格

納されている。

【0061】また、保守用治具3は相手認証に使用する一方関数 $f(R, U)$ を計算機能として有し、相手認証に使用する個別データとして保守用治具識別番号Uを有している。

【0062】まず、保守解体を行う者は保守用治具3の保守用治具識別番号Uを図示せぬ記憶部から読出した後に(図11ステップS31)、外部インタフェース28を通じて制御回路29に端末装置個別番号Rの送信を要求する(図11ステップS32)。

【0063】制御回路29は予めEEPROM30から端末装置個別番号Rを讀出しておき(図11ステップS1)、保守用治具3から端末装置個別番号Rの送信要求を受信すると(図11ステップS2)、その端末装置個別番号Rを保守用治具3に送信する(図11ステップS3)。

【0064】保守用治具3は制御回路29から端末装置個別番号Rを受信すると(図11ステップS33)、記憶部から読出した保守用治具識別番号Uと制御回路29から受信した端末装置個別番号Rとを一方関数 $f(R, U)$ に代入して $M=f(R, U)$ を得る(図11ステップS34)。

【0065】保守用治具3は算出した $M=f(R, U)$ と、記憶部から読出した保守用治具識別番号Uとを外部インタフェース28を通じて制御回路29に送信する(図11ステップS35)。

【0066】制御回路29は保守用治具3から $M=f(R, U)$ と保守用治具識別番号Uとを受信すると(図11ステップS4)、EEPROM30から読出した端末装置個別番号Rと、保守用治具3から受信した保守用治具識別番号Uとを一方関数 $f(R, U)$ に代入して $M'=f(R, U)$ を得る(図11ステップS5)。

【0067】制御回路29は算出した $M'=f(R, U)$ と保守用治具3から受信した $M=f(R, U)$ とを比較する(図11ステップS6)。この結果、算出した $M'=f(R, U)$ と保守用治具3から受信した $M=f(R, U)$ とが異なる値であれば、制御回路29はそれ以降の通信を止め、拒絶状態に移移する(図11ステップS7)。

【0068】また、上記の結果、算出した $M'=f(R, U)$ と保守用治具3から受信した $M=f(R, U)$ とが等しい値であれば、制御回路29は保守用治具3を正当な治具と認めてアクノリッジ信号(ACK)を保守用治具3に送信する(図11ステップS8)。

【0069】保守用治具3は制御回路29からアクノリッジ信号を受信すると(図11ステップS36)、秘匿情報漏洩防止動作の解除要求を外部インタフェース28を通じて制御回路29に送信し(図11ステップS7)、保守動作を開始する(図11ステップS38)。

【0070】制御回路29は保守用治具3から解除要求

を受信すると(図11ステップS9)、秘匿情報漏洩防止動作を解除し(図11ステップS10)、保守動作の受入れ態勢に入る(図11ステップS11)。

【0071】この秘匿情報漏洩防止動作の解除後、上述した端末装置1の解体を電氣的に検出する手段と、磁氣的に検出する手段と、光学的に検出する手段とが夫々端末装置1の解体を検出しても、EEPROM30及びSRAM31に記憶された秘密情報は消去されない。

【0072】尚、上述した相手認証方法については、「高速デジタル署名方式 E S I G N」(岡本龍明・藤岡淳・岩田雅彦著、NTT R&D Vol. 40, No. 5, 1991)の第694頁右欄下から2行目～第695頁右欄6行目記載の「6 相手認証方式」に詳述されている。

【0073】この例では一方向関数 $f(R, U)$ として、端末装置個別番号R及び保守用治具識別番号U各々の各ビットの排他的論理和演算式が用いられているが、秘密性を高めるためには第三者にわからないような複雑な式を一方向関数 $f(R, U)$ として用いればよい。

【0074】上記の図1～図11を用いて本発明の一実施例の動作について以下説明する。本発明の一実施例においては、端末装置1が認識する解体として保守解体及び不正解体の二種類がある。

【0075】この二種類の解体の差は保守用治具3が端末装置1で解体を受理している治具かどうかを判断することで決定される。すなわち、端末装置1の解体作業前に保守用治具3からのアクセス要求に対して端末装置1で相手認証を行い、その結果により保守解体か不正解体かが判断される。

【0076】そこでまず、修理等の目的による保守解体の場合を説明する。端末装置1は製造者から出荷される時点で本発明の一実施例による秘匿情報漏洩防止策が施されている。

【0077】つまり、端末装置1には上述した端末装置1の解体を電氣的に検出する手段と、磁氣的に検出する手段と、光学的に検出する手段とが組込まれ、さらに解体を許可する保守用治具3の相手認証を行うための情報がEEPROM30に格納されている。

【0078】EEPROM30には保守用治具3の相手認証を行うための情報として、端末装置個別番号R(相手認証方式における検証者側乱数)と、保守用治具識別番号U(相手認証方式における証明者側乱数)と、相手認証確認用一方向関数 $f(R, U)$ とが格納されている。

【0079】保守解体を行う場合、その保守解体を行うものは予めこれから行われる解体が保守解体であることを端末装置1の制御回路29に認識させ、秘匿情報漏洩防止動作を解除する必要がある。

【0080】このため、端末装置1及び保守用治具3には相手認証に使用する一方向関数 $f(R, U)$ を計算機

能として有している。また、相手認証に使用する個別データとして端末装置1は端末装置個別番号Rを、保守用治具3は保守用治具識別番号Uを夫々有している。

【0081】上記の番号の桁数や一方向関数式の複雑さによって機械的な錠や電氣的な錠に対して10の10乗以上高い論理的な施錠効果を得ることが可能となる。

【0082】まず、保守解体を行う者は保守用治具3を用いて、端末装置1との間で上述した手順で相手認証を行う。これによって、端末装置1の制御回路29が保守用治具3を正当な治具と認めれば、端末装置1の解体を行ってもEEPROM30及びSRAM31に記憶された秘密情報が消去されることがないので、端末装置1の運用に影響を与えることなく、端末装置1の修理や保守を行うことができる。

【0083】次に、不正解体の場合を説明する。端末装置1が不正解体と認識するのは事前に相手認証が行われない解体全てである。端末装置1の解体が不正に行われる場合、その手段は正規の解体方法とは限らず、筐体の切断等もあり得る。

【0084】そこで、本発明の一実施例では電氣的、磁氣的、光学的の3種類の検出手段によって端末装置1の解体を検出している。以下、上記の3種類の検出手段による検出動作について説明する。

【0085】端末装置1の解体を電氣的に検出する場合について図10を用いて説明する。不正解体を行う者はプリント配線基板2を露出させ、内部回路動作及びそれに関わるデータを解析することを目的に解体を行うので、筐体前面部4及び筐体後面部5をプリント配線基板2から分離しようとする。

【0086】このような意図を持って解体が行われる場合、特に筐体の切断等の方法によらなければ、筐体前面部4を筐体後面部5にネジ止めしているネジ9c～9fを取外す必要が生ずる。

【0087】これらのネジ9c～9fを取外すと、筐体後面部5にネジ9a, 9bで固定されたプリント配線基板2に半田付けされたバネ状の金具21a, 21cによって筐体前面部4がプリント配線基板2から1mm程度持ち上がる。

【0088】すると、バネ状の金具21a, 21cの他端がプリント配線基板2上の銅箔部12から離れ、バネ状の金具21a, 21cの電位がプリント配線基板2のグランド電位から切離されて異なる電位を持つことになる。

【0089】電位変換回路22a, 22cはバネ状の金具21a, 21cの電位変化を検出すると、その検出結果を検出/非検出の二値信号に変換して制御回路29に通知する。

【0090】よって、制御回路29は保守用治具3により秘匿情報漏洩防止動作の解除が行われていないときに、電位変換回路22a, 22cからバネ状の金具21

a, 21cの電位変化を検出が通知されると、EEPROM30及びSRAM31に記憶された秘密情報を消去する。

【0091】もちろん、正規の手段によらず、筐体後面部5が筐体前面部4よりも先にプリント配線基板2から分離された場合も、上記の動作と同様に、端末装置1の解体を検出することはバネ状の金具21b, 21dによって可能である。

【0092】次に、端末装置1の解体を磁気的に検出する場合について図9を用いて説明する。不正解体を行う者はプリント配線基板2を露出させようとすると、端末装置1の構造上、まず筐体前面部4をプリント配線基板2から分離させなければならない。

【0093】正規の手段に準じた方法にて端末装置1の解体を行う場合、まず電池パック6を筐体後面部5から取外した後に、筐体後面部5からネジ9c~9fを取外す。その後に、筐体前面部4を頭頂部の筐体嵌合用の爪4aを支点として筐体後面部5から分離させる。

【0094】そうすると、筐体前面部4内面に取付けた磁石23がホール素子24における磁界検出範囲から外れてしまうので、ホール素子24は磁石23の磁界変化を検出し、その磁界変化を電気信号に変換して出力する。電位変換回路25はホール素子24の出力から磁石23の磁界変化を検出し、その検出結果を検出/非検出の二値信号に変換して制御回路29に通知する。

【0095】よって、制御回路29は保守用治具3により秘匿情報漏洩防止動作の解除が行われていないときに、電位変換回路25からホール素子24による磁石23の磁界変化の検出が通知されると、EEPROM30及びSRAM31に記憶された秘密情報を消去する。

【0096】また、端末装置1の解体を光学的に検出する場合について図1~図4を用いて説明する。不正解体を行う者はプリント配線基板2を露出させようとすると、端末装置1の構造上、筐体前面部4または筐体後面部5をプリント配線基板2から分離させなければならない。

【0097】正規の手段に準じた方法にて端末装置1の解体を行う場合、まず電池パック6を筐体後面部5から取外した後に、筐体後面部5からネジ9c~9fを取外す。その後に、筐体前面部4を頭頂部の筐体嵌合用の爪4aを支点として筐体後面部5から分離させる。

【0098】そうすると、プリント配線基板2上のフォトトランジスタ26a~26dのうちいずれか(1つでもあるいは複数でもよい)に外部から光線が照射され、光線が照射されたフォトトランジスタ26a~26dの出力が変化する。

【0099】電位変換回路27a~27dはフォトトランジスタ26a~26dの出力の変化を検出し、その検出結果を検出/非検出の二値信号に変換して制御回路29に通知する。

【0100】よって、制御回路29は保守用治具3により秘匿情報漏洩防止動作の解除が行われていないときに、電位変換回路27a~27dからフォトトランジスタ26a~26dの出力の変化が通知されると、EEPROM30及びSRAM31に記憶された秘密情報を消去する。

【0101】もちろん、正規の手段によらず、筐体後面部5を筐体前面部4よりも先にプリント配線基板2から分離した場合や筐体前面部4または筐体後面部5の一部を切取ったりあるいは切断した場合も、上記の動作と同様に、端末装置1の解体を検出することはフォトトランジスタ26a~26dによって可能である。

【0102】上述した3種類の検出手段によって端末装置1の解体の検出情報は夫々制御回路29に通知される。制御回路29は各回路から通知された検出情報の組合せや通知順序等によって通知原因が落下等の偶発的な事故によるものか、あるいは不正解体によるものかを判断区別し、夫々に対応して処理を行う。

【0103】これは端末装置1の運用において、落下事故等による衝撃や人もしくは物の下敷きになって荷重を受けることで、筐体の損傷等から不正解体と誤認識し、誤ってEEPROM30及びSRAM31に記憶された秘密情報を消去しないようにするためである。この判断を行うことで、偶発的な事故等による筐体の破損を検出することが可能となる。

【0104】制御回路29が導き出す判断結果として偶発的な事故等による破損と判断した場合、上記3種類の検出手段からの検出情報によって、「運用可能及び加入者に対して修理要求」あるいは「運用不可(EEPROM30の記憶情報消去)」のうちいずれかの処理を実行する。

【0105】これは回線網の立場あるいは加入者の立場から見て、筐体が破損した端末装置1の運用が他に悪影響を与える危険があるので、制御回路29はこのような対応を実行する。

【0106】また、制御回路29は導き出す判断結果として不正解体による破損と判断した場合、「運用不可(EEPROM30及びSRAM31の記憶情報消去)」の処理を実行する。

【0107】このように、バネ状の金具21a~21dや筐体前面部4及び筐体後面部5の内面の蒸着膜の仲立ちで、筐体とプリント配線基板2とが電気的に同一電位であること、言い換えれば正規な状態で接触していることを検出することによって、プリント配線基板2上の各電子回路への不正なアクセスを認識することが可能となるため、不正アクセス検出専用の機械的あるいは電気的な機構を使用せずに、不正アクセスを認識することができる。

【0108】また、不正アクセスの電気的な検出信号や光学的な検出信号、及び磁気的な検出信号を組合せて用

いることで、筐体の破壊や解体が故意か事故かを判別し、軽微な機構的損傷であればEEPROM30やSRAM31の秘密情報を保持して端末装置1の運用を可能としながら、使用者に対して修理要求をすることができ

る。
【0109】一方、筐体の破壊や解体が悪意の第三者による不正なアクセスと判断した場合にはEEPROM30やSRAM31の秘密情報を消去し、以後の端末装置1の運用を不可能として情報の漏洩を防ぐことができ

る。
【0110】さらに、端末装置1の解体の正当性証明のための相手認証に錠等の機構的な手段を使用せずに、外部インタフェース28等の通信回路を用いた論理的な相手認証方式を使用することで、軽量小型で、量産や保守の簡便さを実現することができる。これによって、使用上、落下事故が生じる確率が非常に高い移動体通信端末装置に適用することが可能となる。

【0111】

【発明の効果】以上説明したように本発明によれば、秘密情報を記憶するメモリを含む電子回路に対する外部からのアクセス許可要求の適否を判定するとともに、この電子回路が搭載されたプリント配線基板を収納する外部筐体の解体の有無を複数の異なる手段で検出し、これらの判定結果及び検出結果に基づいて外部筐体の不正な解体と判断したときに秘密情報をメモリから消去することによって、機械的な手段を用いることなく、不正アクセスの認識を可能とすることができるという効果がある。

【図面の簡単な説明】

【図1】本発明の一実施例の構成を示すブロック図である。

【図2】本発明の一実施例の組立図である。

【図3】組立て状態における図2のAA線に沿う矢視方向の断面図である。

【図4】組立て状態における図2のBB線に沿う矢視方向の断面図である。

【図5】図2の金具を示す斜視図である。

【図6】図5のCC線に沿う矢視方向の断面図である。

【図7】図2のパネ状の金具の取付け状態を示す斜視図である。

【図8】図7のDD線に沿う矢視方向の断面図である。

【図9】(a)は図2のプリント配線基板と筐体前面部と筐体後面部とを組立てる前の磁石及びホール素子の状態を示す図、(b)は図2のプリント配線基板と筐体前面部と筐体後面部とを組立てた後の磁石及びホール素子の状態を示す図である。

【図10】(a)は図2のプリント配線基板と筐体前面部と筐体後面部とを組立てる前のパネ状の金具の状態を示す図、(b)は図2のプリント配線基板と筐体前面部と筐体後面部とを組立てた後のパネ状の金具の状態を示す図である。

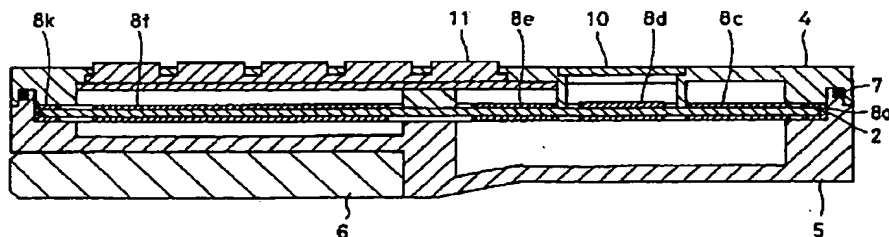
【図11】図1の端末装置における相手認証方法の手順を示すフローチャートである。

【図12】従来例の構成を示すブロック図である。

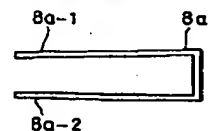
【符号の説明】

- 1 端末装置
- 2 プリント配線基板
- 3 保守用治具
- 4 筐体前面部
- 5 筐体後面部
- 6 電池パッケージ
- 7 密閉用ゴムパッキン
- 8 a～8 l 金具
- 9 a～9 f ネジ
- 12 銅箔部
- 21 a～21 d パネ状の金具
- 22 a～22 d, 25, 27 a～27 d 電位変換回路
- 23 磁石
- 24 ホール素子
- 26 a～26 d フォトトランジスタ
- 28 外部インタフェース
- 29 制御回路
- 30 EEPROM
- 31 SRAM

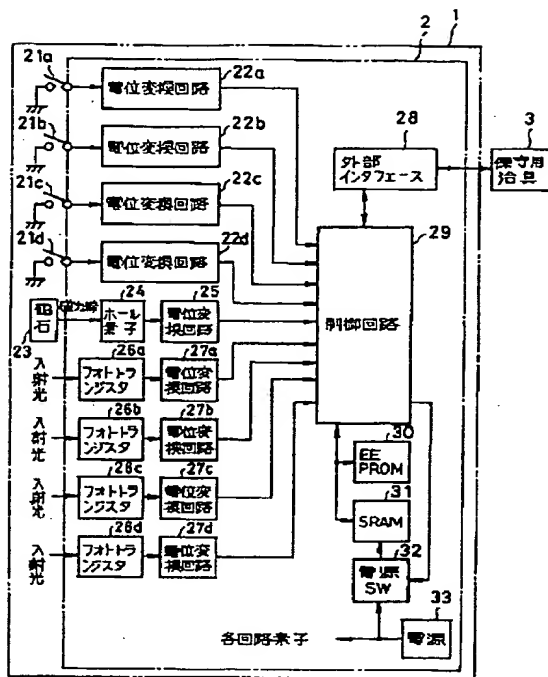
【図3】



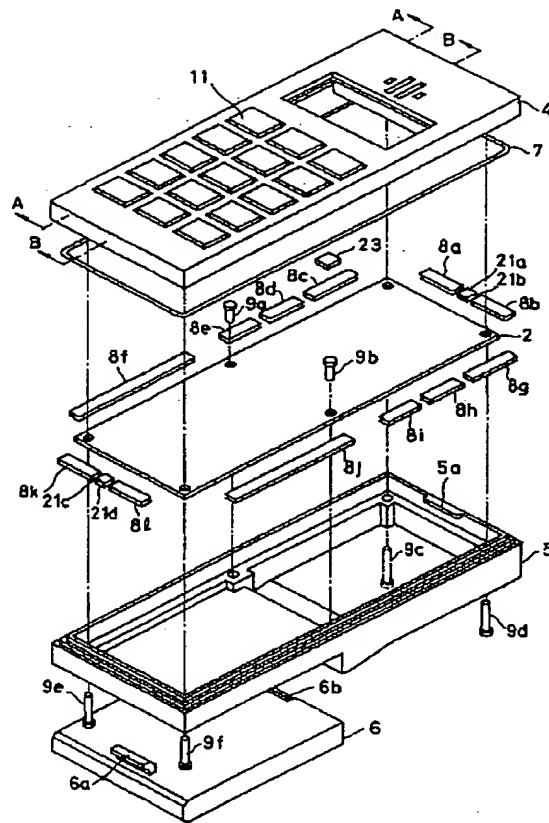
【図6】



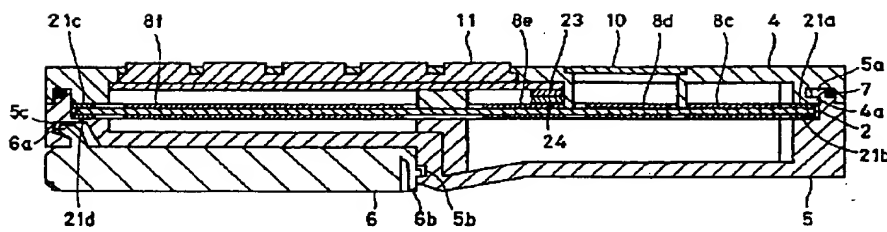
【図1】



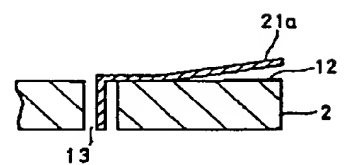
【図2】



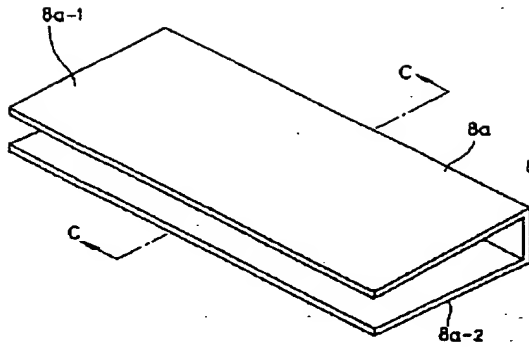
【図4】



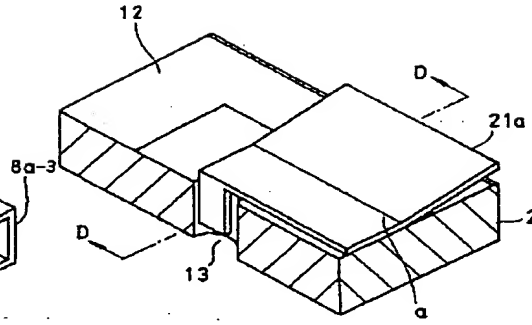
【図8】



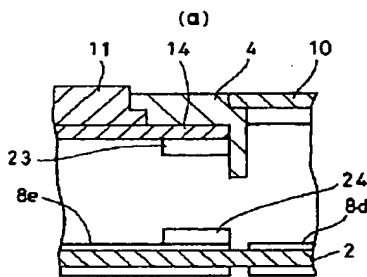
【図5】



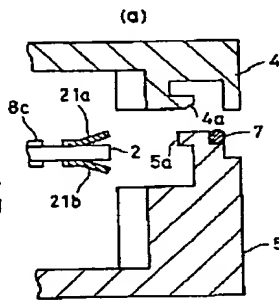
【図7】



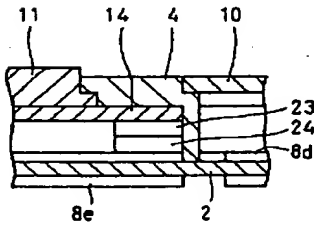
【図9】



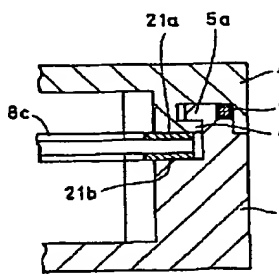
【図10】



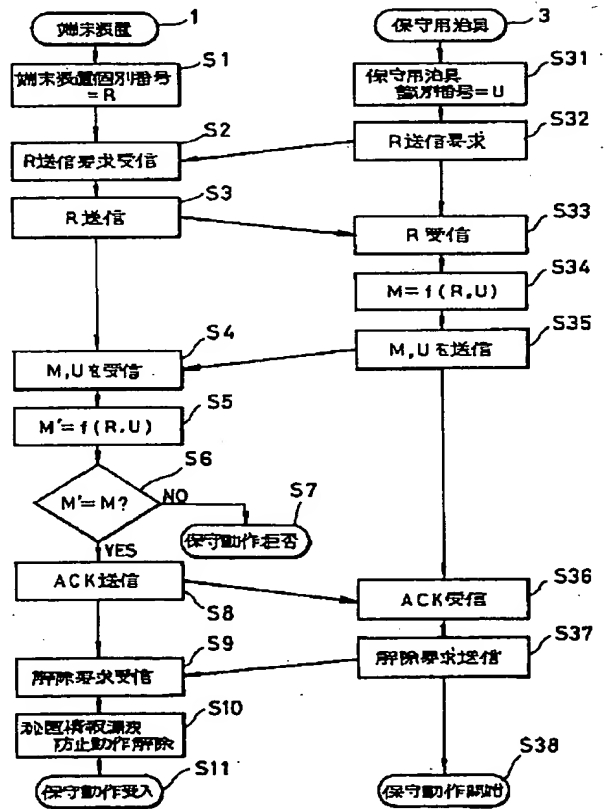
(b)



(b)



【図11】



【図 12】

